4. Poison the logs

As usual the objective is to capture the flag however this time the flag would be set to a random path on the server. to get it you will need to at least have a decent shell access .

- Target Machine: Cyber - WebSec 0x07
- Main Endpoint: `http://web0x07.hbtn/find_your_shell/`

```
Useful instructions:
1. Investigate what files you have permission to access.
2. Check paths under root
```

Repo:

- GitHub repository: `holbertonschool-cyber_security`
- Directory: `web_application_security/0x07_file_inclusion`
- File: `4-flag.txt`